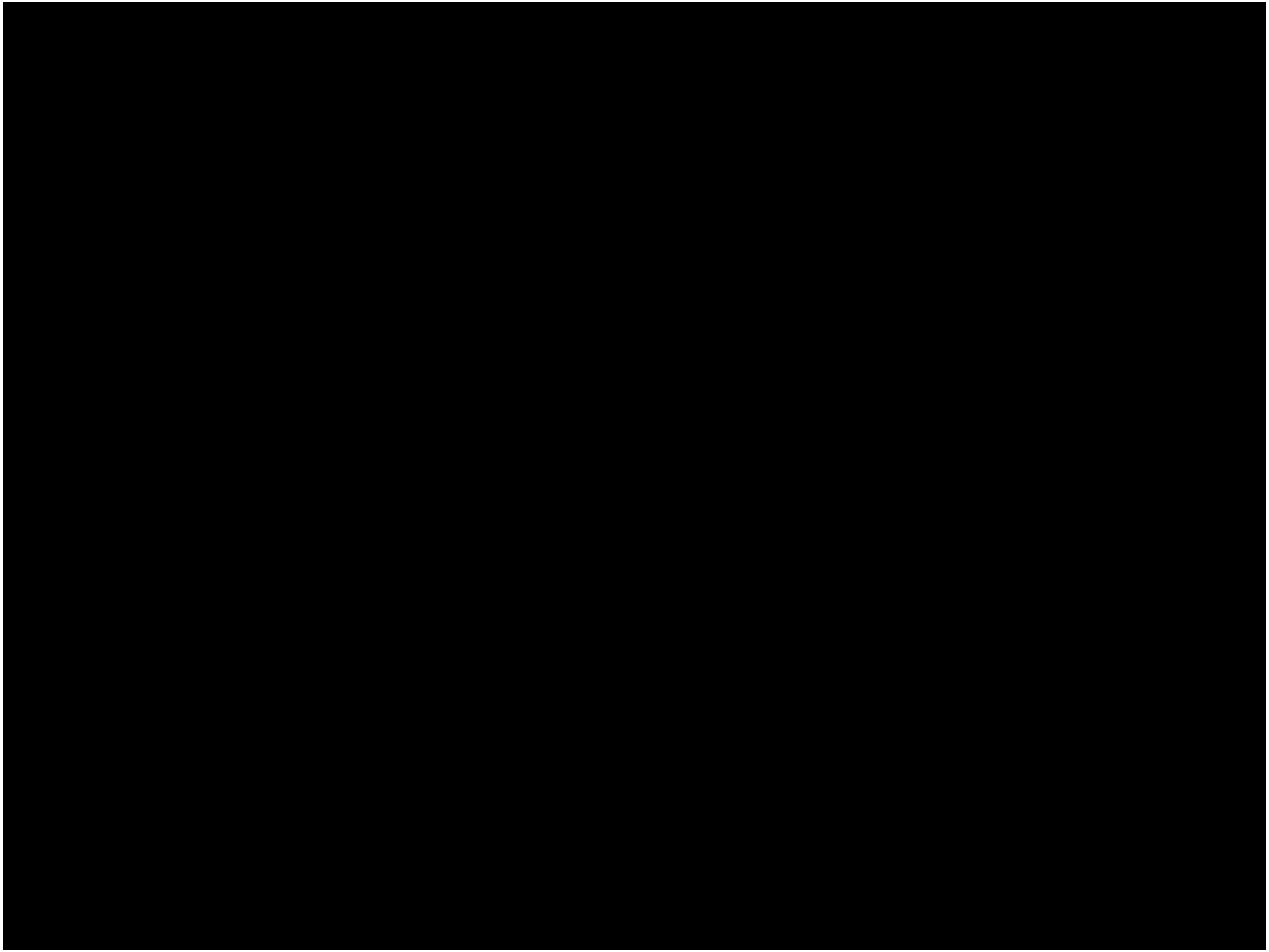
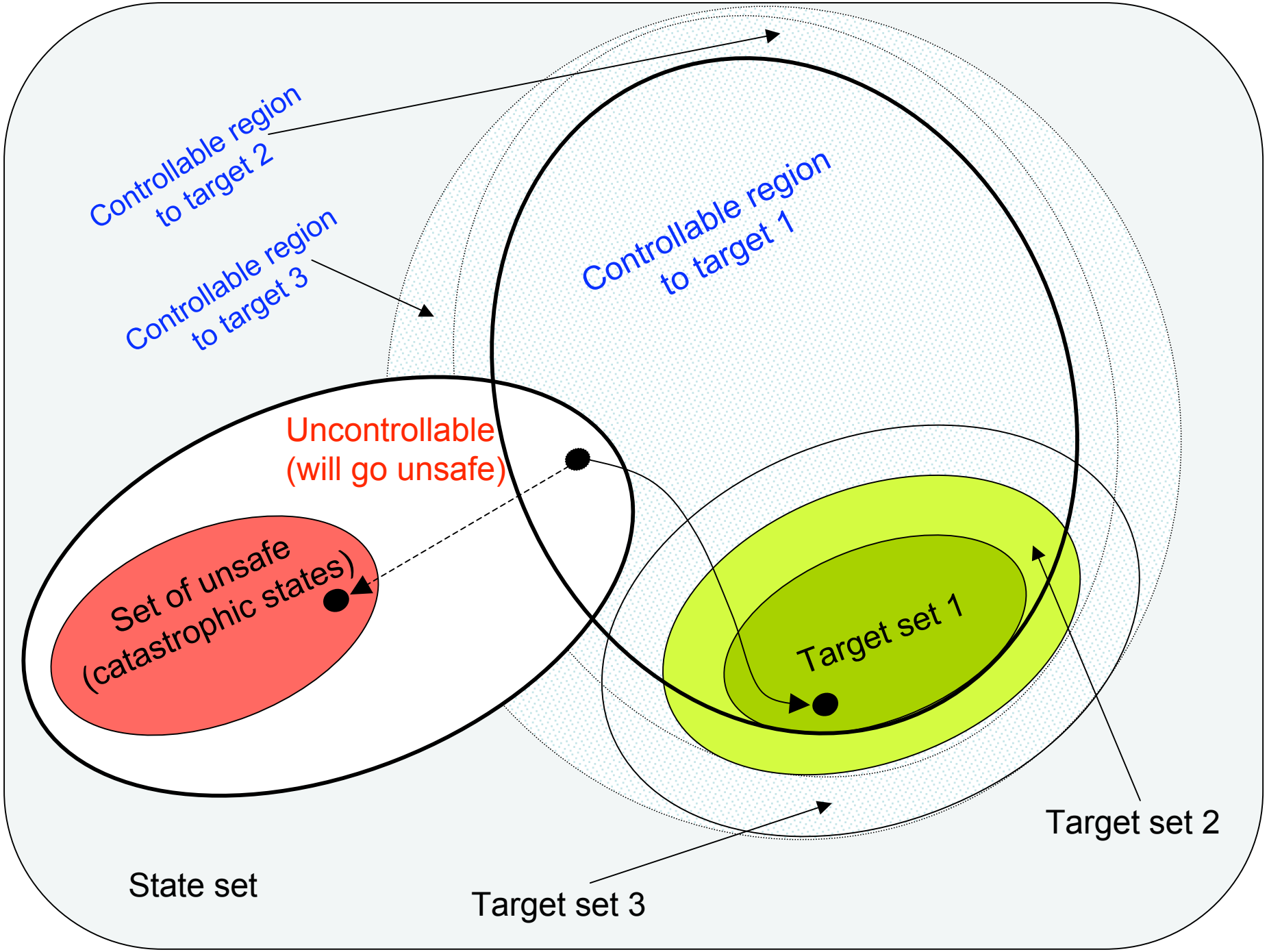
Some Aspects of Procedure Verification and Synthesis

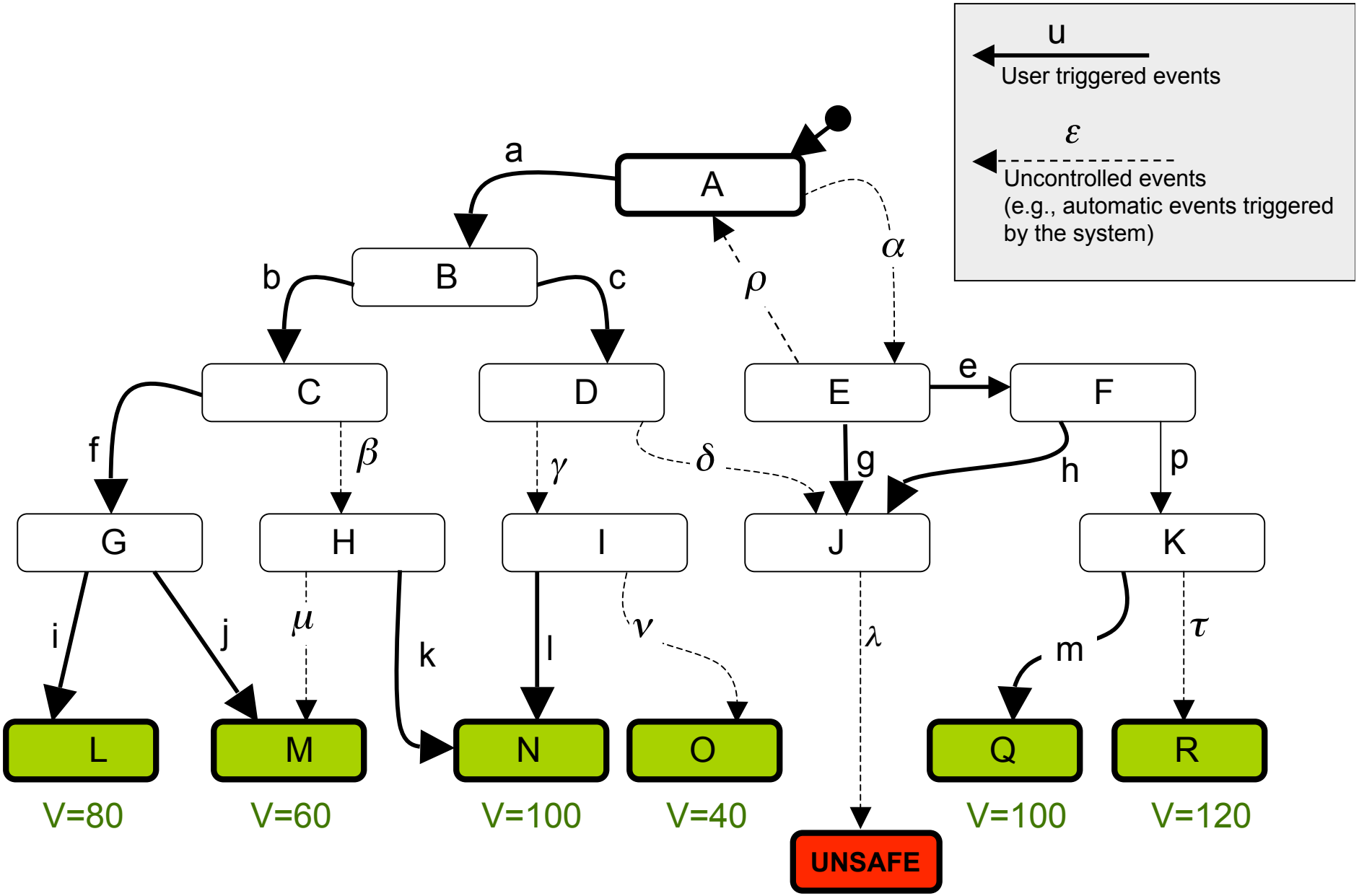
Asaf Degani
NASA Ames Research Center (Code IC)
adegani@mail.arc.nasa.gov

Michael Heymann
San Jose State University/Technion, Israel
heymann@cs.technion.ac.il



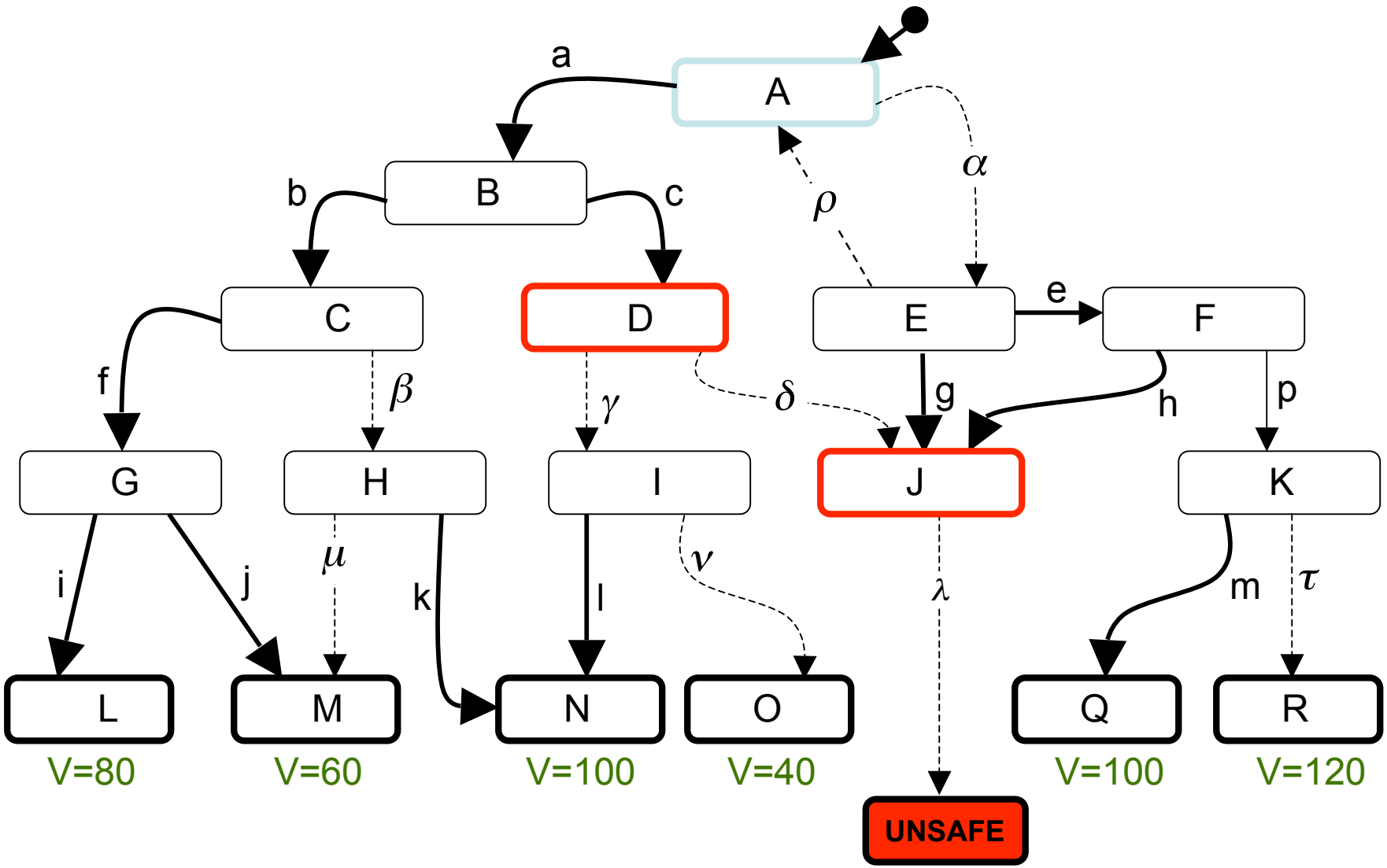

Controllable region
to target 2
Controllable region
to target 3
Controllable region
to target 1
Uncontrollable
(will go unsafe)
Set of unsafe
(catastrophic states)
Target set 1
Target set 2
State set
Target set 3

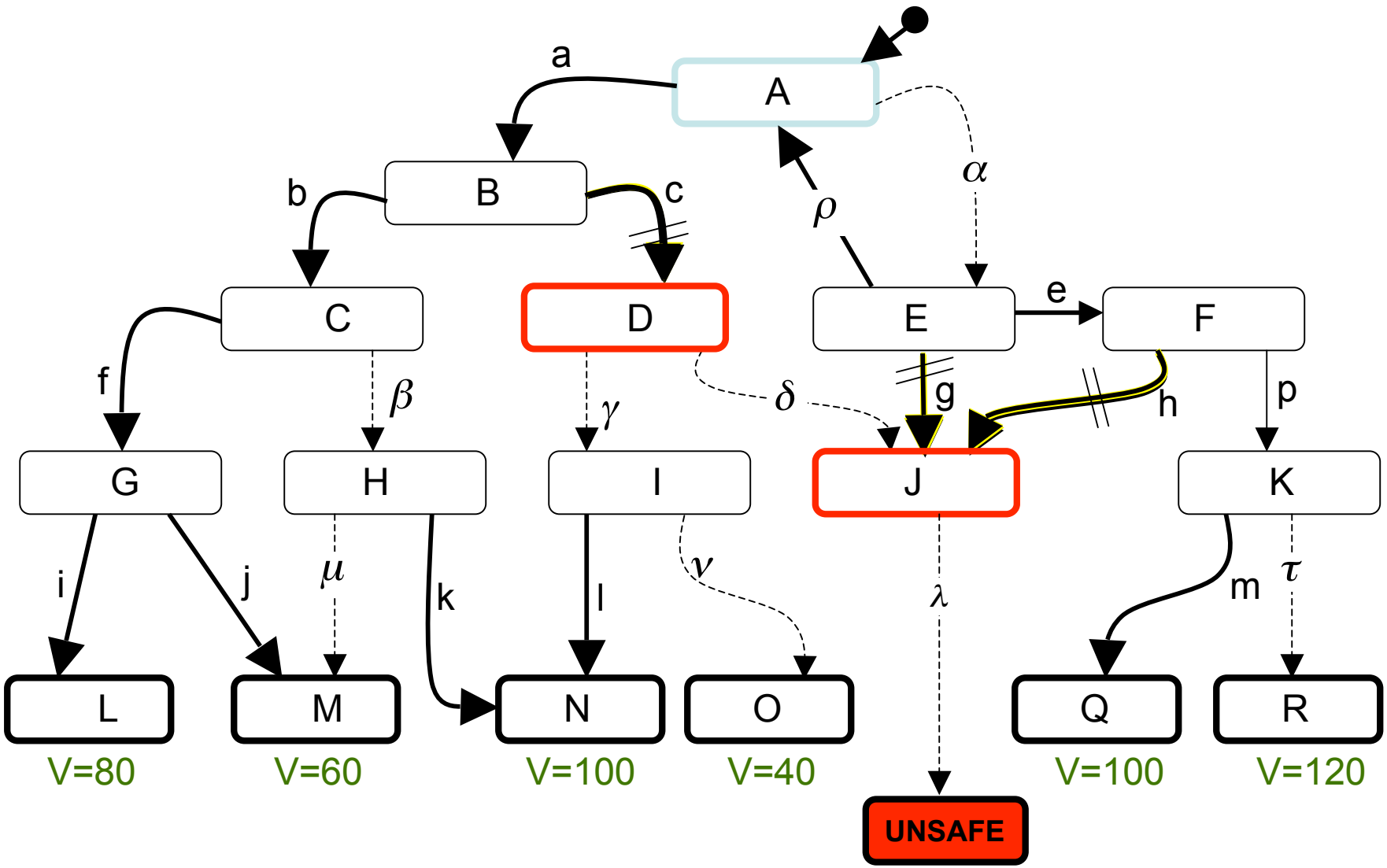
A given (say aircraft) sub-system



First objective:

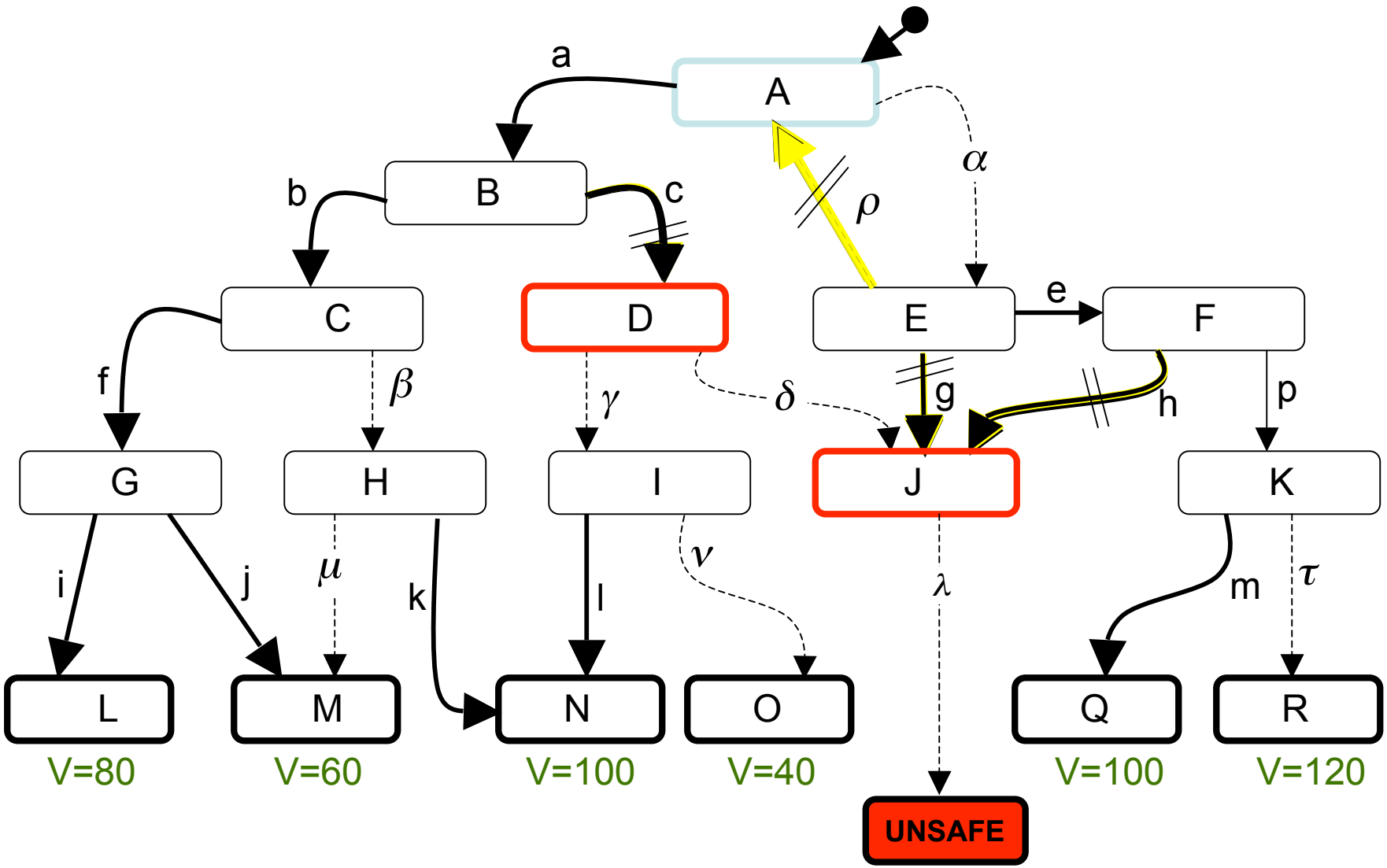
Preventing Catastrophe

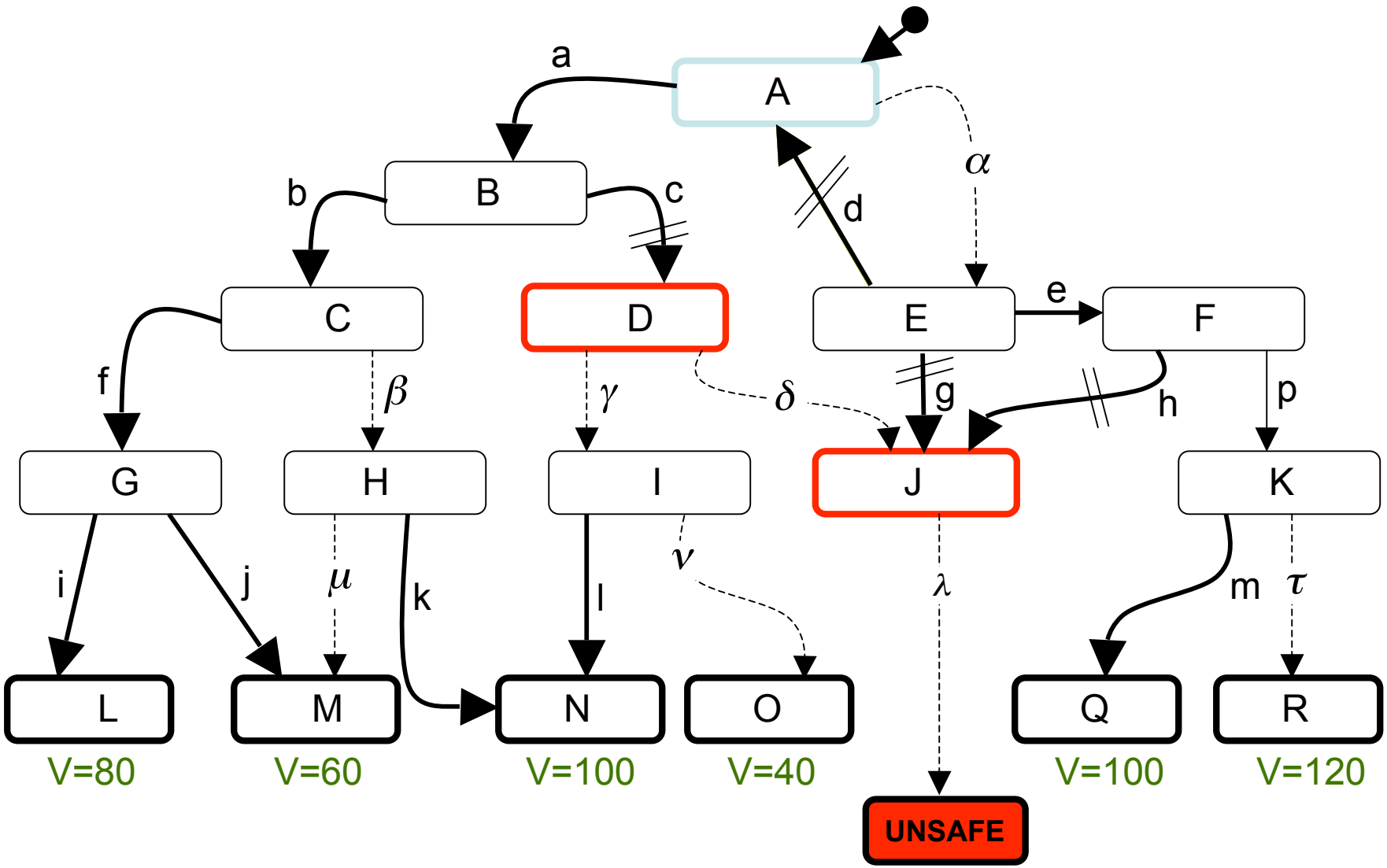

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
Q
R
a
b
c
e
f
g
h
i
j
k
l
m
p
α
β
γ
δ
ρ
μ
ν
λ
τ
V=80
V=60
V=100
V=40
V=100
V=120
UNSAFE


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
Q
R
UNSAFE
a
b
c
d
e
f
g
h
i
j
k
l
m
p
α
β
γ
δ
ρ
μ
ν
λ
τ
V=80
V=60
V=100
V=40
V=100
V=120

Second objective:

Begin stabilization and recovery sequences (with guaranteed termination)


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
Q
R
a
b
c
α
ρ
e
f
β
γ
δ
g
h
p
i
j
μ
k
l
ν
λ
m
τ
V=80
V=60
V=100
V=40
V=100
V=120
UNSAFE


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
Q
R
a
b
c
d
e
f
g
h
i
j
k
l
p
m
α
β
γ
δ
μ
ν
λ
τ
V=80
V=60
V=100
V=40
UNSAFE
V=100
V=120

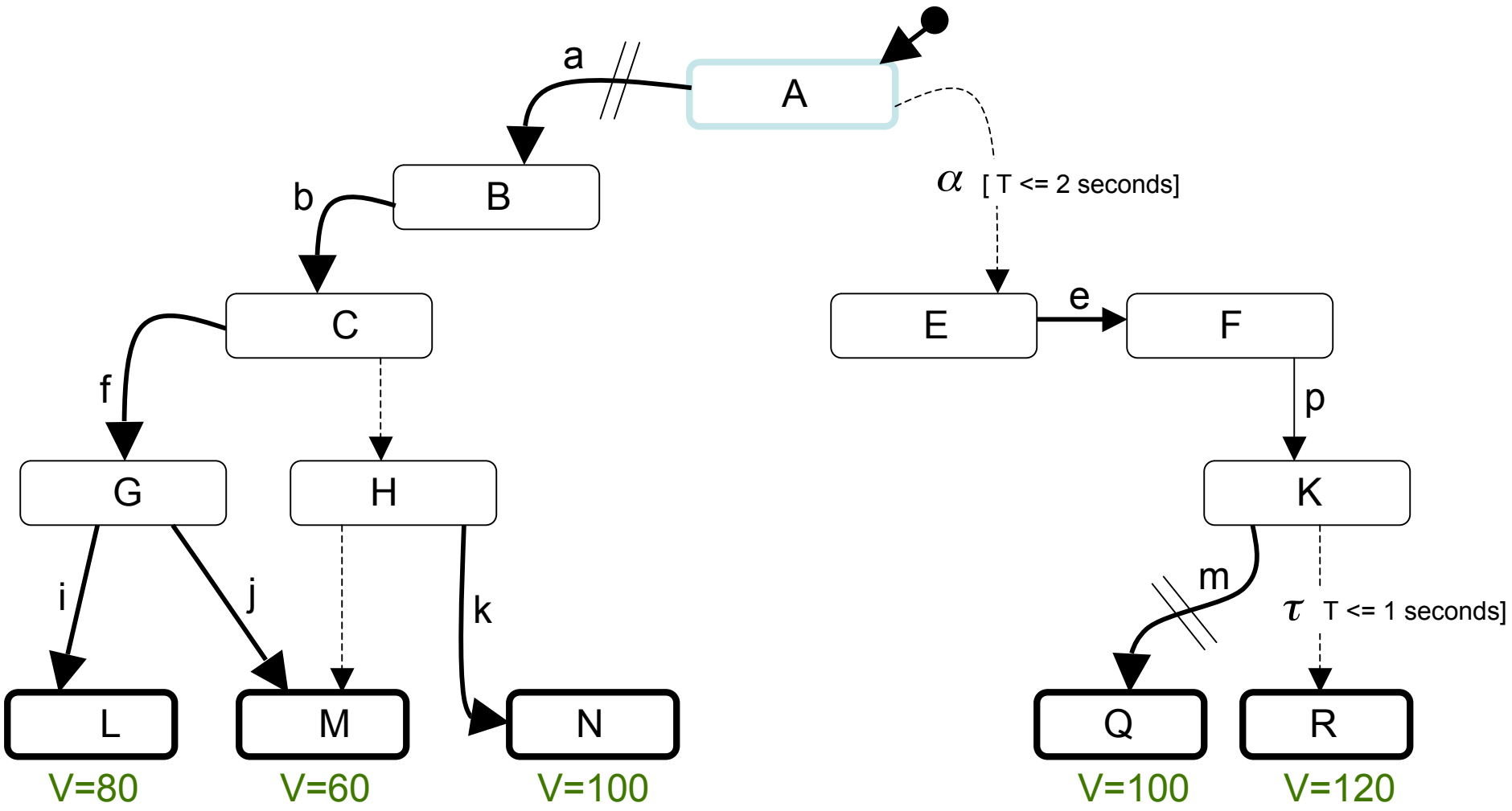
Third objective:

Generating recovery sequences
(by maximizing least return)

Case 1:

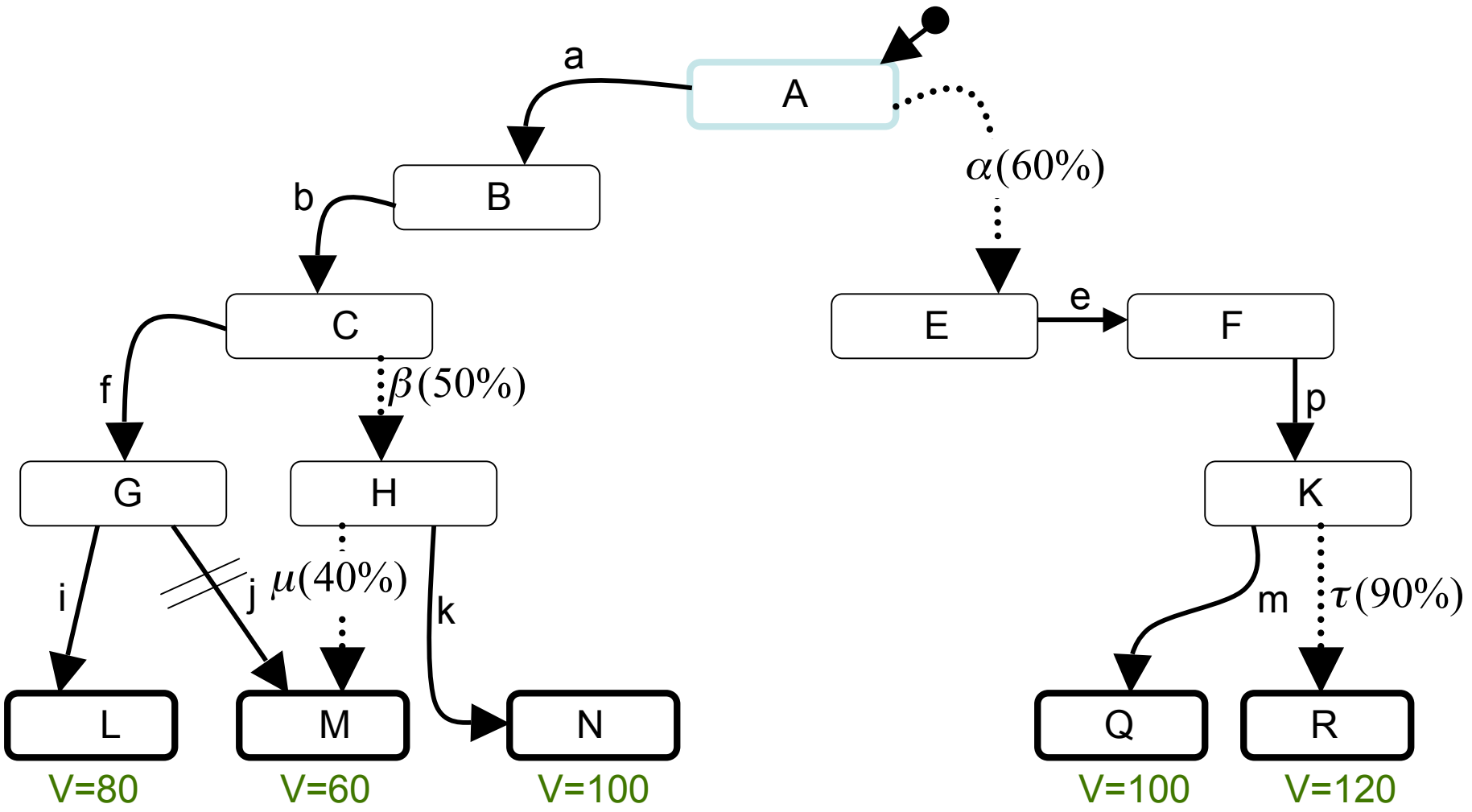
Automatic and time bounded events

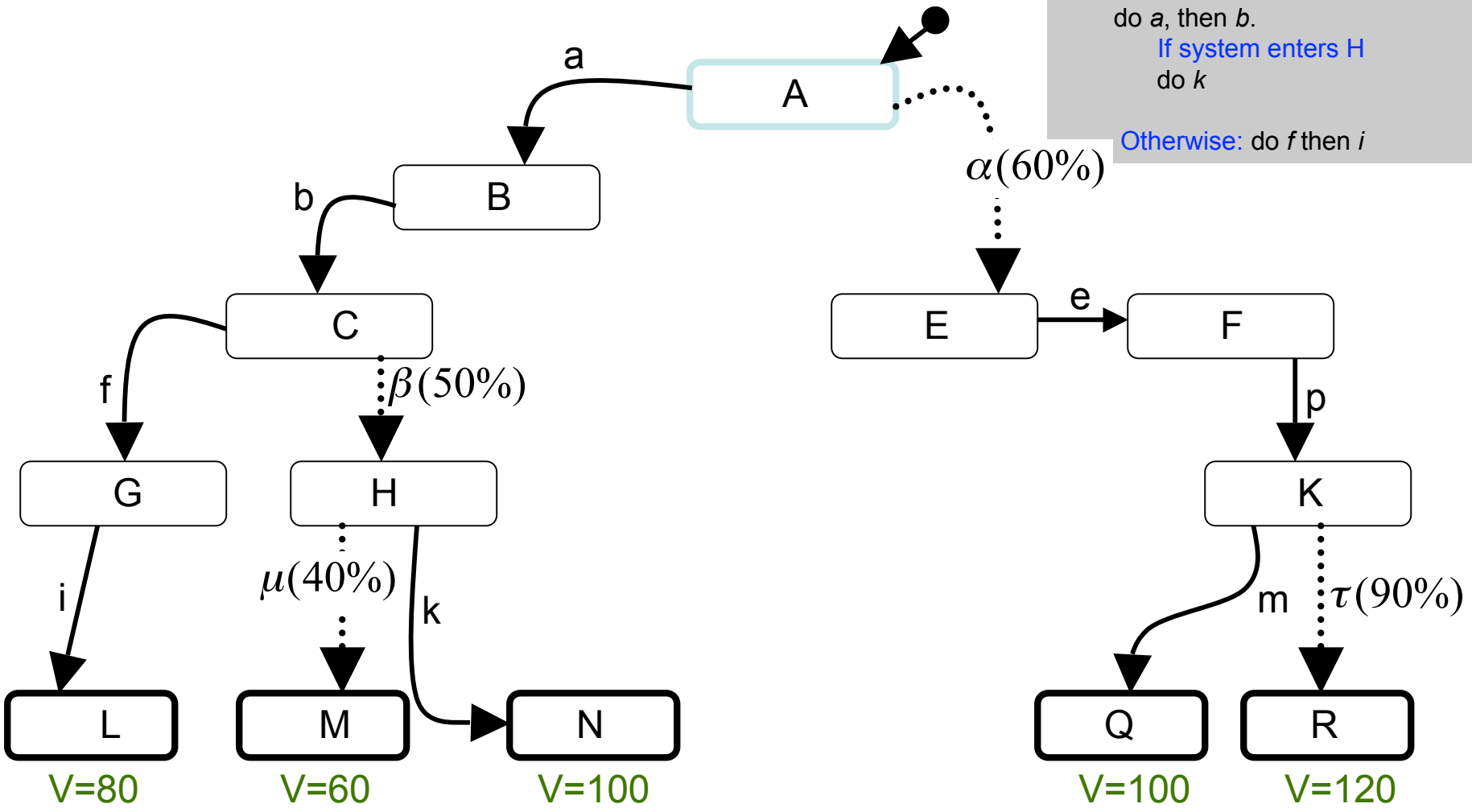
Procedure: Wait until α happens (system enters E) and then execute Event *e* and then *p*.

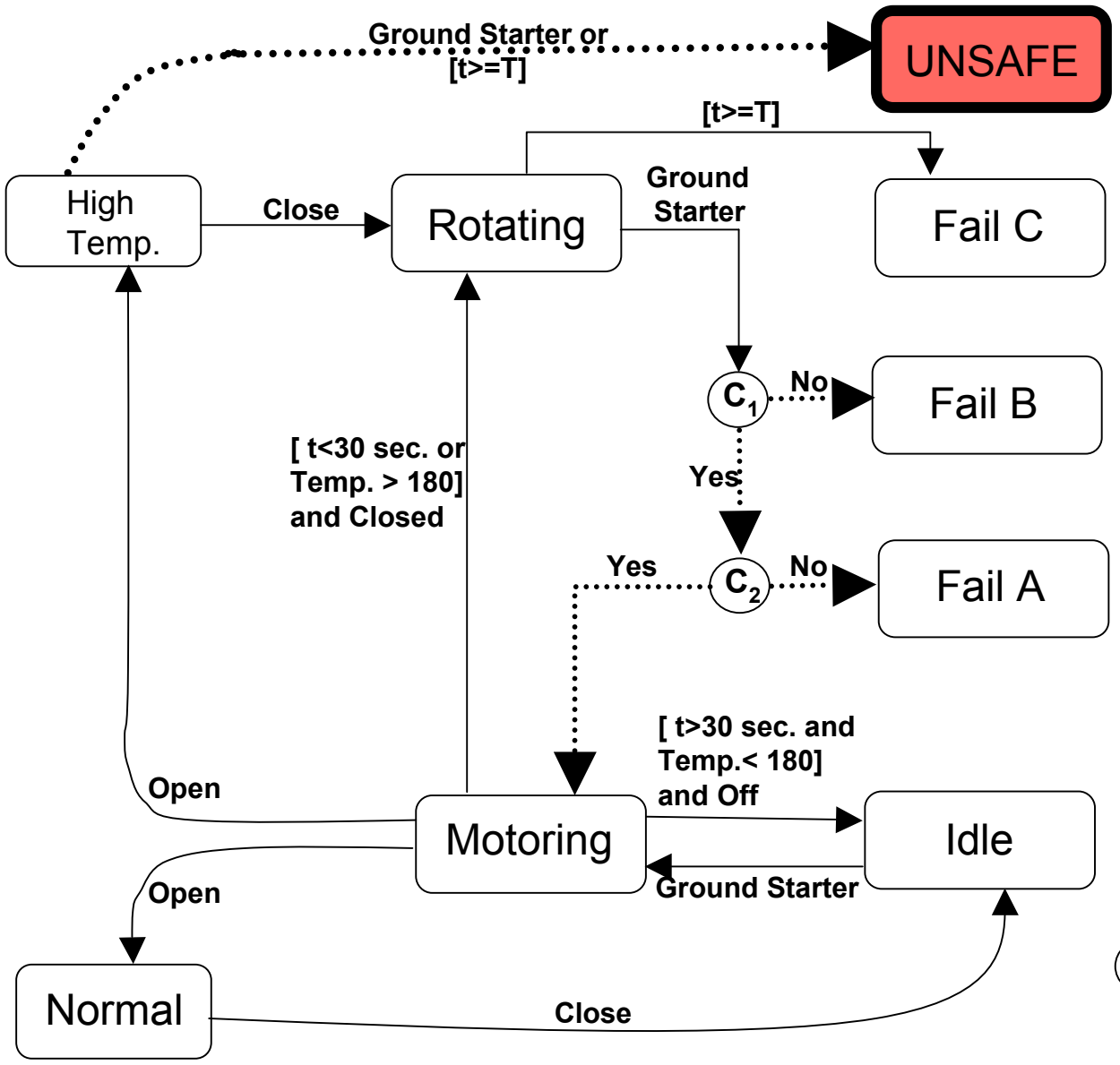


Case 2:

Dotted events are triggered by
the environment
(i.e., they *may* or *may not* occur)


A
a
B
b
C
f
G
i
j
L
V=80
H
β(50%)
μ(40%)
M
V=60
k
N
V=100
α(60%)
E
e
F
p
K
m
Q
V=100
τ(90%)
R
V=120


PROCEDURE:
If system enters state E
execute event e and then p.
if system is stuck in state K
execute event m
Otherwise:
do a, then b.
If system enters H
do k
Otherwise: do f then i
A
B
C
E
F
G
H
K
L
M
N
Q
R
a
b
f
e
p
i
k
m
α(60%)
β(50%)
μ(40%)
τ(90%)
V=80
V=60
V=100
V=100
V=120



IMMEDIATE ACTION

FUEL CONTROL SWITCH . . . . . CUTOFF

ENGINE START SELECTOR. . . . . .GND

Motor for 30 seconds or until EGT is below 180, whichever is longer (unless no oil pressure).

NOTE

If starter cutout has occurred, reselect GND when N2 is below 20%

If problem was other raped EGT rise:

ENGINE START SELECTOR. . . . . .OFF

C_1 = Oil Pressure OK

C_2 =[N2<=20%]

Research on verification/synthesis of procedures